Listing of the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1.   (Currently Amended) A method for authorizing a command from a user received at a network device separate and distinct from an Authentication, Authorization, and Accounting (AAA) server, the method including:

establishing an access control protocol ~~RADIUS~~ session with the user;

receiving a user profile for the user at the network device from a AAA server, the user profile containing information regarding which commands the user is authorized to execute, the information including a command set described by regular expressions;

storing the user profile in a memory accessible by the network device;

receiving the command from the user;

comparing the command to said command set contained in said user profile; and

~~determining whether the command is authorized based on the information in the user profile stored in the memory; and~~

authorizing the command if the command is contained in said command set ~~or rejecting the command in response to said determining~~.

2.   (Original) The method of claim 1, wherein the network device is a Network Access Server (NAS).

3.   (Currently Amended) The method of claim 1, further including purging said user profile from said memory when said access control protocol ~~RADIUS~~ session is terminated.

4.   (Currently Amended) The method of claim 1, wherein said <u>access control protocol</u>

<u>session is a RADIUS session</u>~~determining includes comparing said command to a command set~~

~~contained in said user profile and said authorizing includes authorizing the command if it is~~

~~contained in said command set~~.

5.   (Currently Amended) The method of claim <u>1</u>[4], wherein said command set is a list of

previously authorized commands.

6.   (Currently Amended) The method of claim <u>1</u>[4], wherein said command set is described

by regular expressions.

7.   (Currently Amended) An apparatus for authorizing a command from a user received at a

network device separate and distinct from an Authentication, Authorization, and Accounting

(AAA) server, the apparatus including:

        a RADIUS session initiator;

        a user profile receiver coupled to said RADIUS session initiator and coupled to a AAA

server;

        a memory <u>containing a user profile having a command set</u>;

        a user profile storer coupled to said user profile receiver and said memory;

        a command receiver;

        <u>a command set comparer coupled to said memory and to said command receiver</u>~~an~~

~~authorized command determiner coupled to said command receiver and to said memory~~; and

        a command authorizer coupled to said <u>command set comparer</u> ~~authorized command~~

~~determiner~~.

8.   (Original) The apparatus of claim 7, wherein the network device is a Network Access Server (NAS).

9.   (Original) The apparatus of claim 7, further including a user profile purger coupled to said memory.

10.   (Canceled)

11.   (Currently Amended) The apparatus of claim 7 ~~10~~, wherein said command set is a list of previously authorized commands.

12.   (Currently Amended) The apparatus of claim 7 ~~10~~, wherein said command set is described by regular expressions.

13.   (Currently Amended) An apparatus for authorizing a command from a user received at a network device separate and distinct from an Authentication, Authorization, and Accounting (AAA) server, the method including:

        means for establishing <u>an access control protocol</u> ~~RADIUS~~ session with the user;

        means for receiving a user profile for the user at the network device from a AAA server, the user profile containing information regarding which commands the user is authorized to execute, the information including a command set described by regular expressions;

        means for storing the user profile in a memory accessible by the network device;

        means for receiving the command from the user;

means for <u>comparing the command to said command set contained in said user profile</u> ~~determining whether the command is authorized based on the information in the user profile~~ ~~stored in the memory~~; and

means for authorizing <u>the command if the command is contained in said command set</u> ~~or~~ ~~rejecting the command in response to said determining~~.

14. (Original) The apparatus of claim 13, wherein the network device is a Network Access Server (NAS).

15. (Currently Amended) The apparatus of claim 13, further including means for purging said user profile from said memory when said <u>access control protocol</u> ~~RADIUS~~ session is terminated.

16. (Currently Amended) The apparatus of claim 13, wherein said <u>access control protocol</u> <u>session is a RADIUS session</u> ~~means for determining includes means for comparing said~~ ~~command to a command set contained in said user profile and said means for authorizing~~ ~~includes means for authorizing the command if it is contained in said command set~~.

17. (Currently Amended) The apparatus of claim <u>13</u> ~~16~~, wherein said command set is a list of authorized commands.

18. (Currently Amended) The apparatus of claim <u>13</u> ~~16~~, wherein said command set is described by regular expressions.

19.   (Currently Amended) A program storage device readable by a machine, tangibly

embodying a program of instructions executable by the machine to perform a method for

authorizing a command from a user received at a network device separate and distinct from an

Authentication, Authorization, and Accounting (AAA) server, the method including:

establishing a~~n~~ access control protocol ~~RADIUS~~ session with the user;

receiving a user profile for the user at the network device from a AAA server, the user

profile containing information regarding which commands the user is authorized to execute, the

information including a command set described by regular expressions;

storing the user profile in a memory accessible by the network device;

receiving the command from the user;

comparing the command to said command set contained in said user profile; and

~~determining whether the command is authorized based on the information in the user~~

~~profile stored in the memory; and~~

authorizing the command if the command is contained in said command set ~~or rejecting~~

~~the command in response to said determining~~.